Fault Management Algorithm Risk Assessment for the NASA Space Launch System

January 24, 2024, Session 11C Fault Tree Analysis

William Maul, HX5 LLC

Yunnhon Lo, PhD, Jacobs

Edmond Wong, NASA Glenn Research Center

RAMS 2024

Overview and Outline

Space Launch System (SLS) Artemis II Fault Management (FM) Detection Risk Assessment

Presentation Outline

- Background
- Analysis Scope
- Analysis Process
- Analysis Refinements
- Current Assessment Status

SLS FM Risk Assessment Background

SLS Fault Management (FM) function set assesses and responds to off-nominal conditions

- Objectives - Crew Safety and Mission Success
  - Annunciating Conditions to flight crew and mission support personnel (Cautions and Warnings)
  - Performing predetermined operational responses (Aborts, Redundancy Management and Safing Responses)

FM Risk Assessment

- False Positive (FP) – FM initiating an unwarranted response
- False Negative (FN) – FM not responding when needed

SLS FM Risk Assessment Background (continued 2/3)

FM function

- Detection – monitor for specific off-nominal conditions
- Response - transmit and perform the response actions

FM Detection Function

- Threshold-Based Assessment
  - Applicable mainly to functions that monitor continuous state variables.
  - Limits, Persistence, Timing
  - Requires physics-based modeling and simulations
- Non-Threshold-Based Assessment
  - Detection system reliability

SLS FM Risk Assessment Background (continued 3/3)

Objective: Estimate the FP and FN risks for the SLS FM detection functions individually and as a suite

- Individual risk assessment
  - Verify detection architecture and function selection,
  - Identify potential areas of improvement in detection architecture or software development.
- Consolidated risk assessments feed into SLS-level and Cross-Program Loss of Mission (LOM)/Loss of Crew (LOC) risk assessments, and SLS abortability assessments.

SLS FM Detection Risk Assessment Analysis Scope

Analysis based on

- SLS Block 1 crewed-vehicle design – includes the Solid Rocket Boosters, Core Stage element, and the Core Stage Engines.
- Integrated vehicle prelaunch and ascent timelines for the Artemis II mission.

Analysis excludes

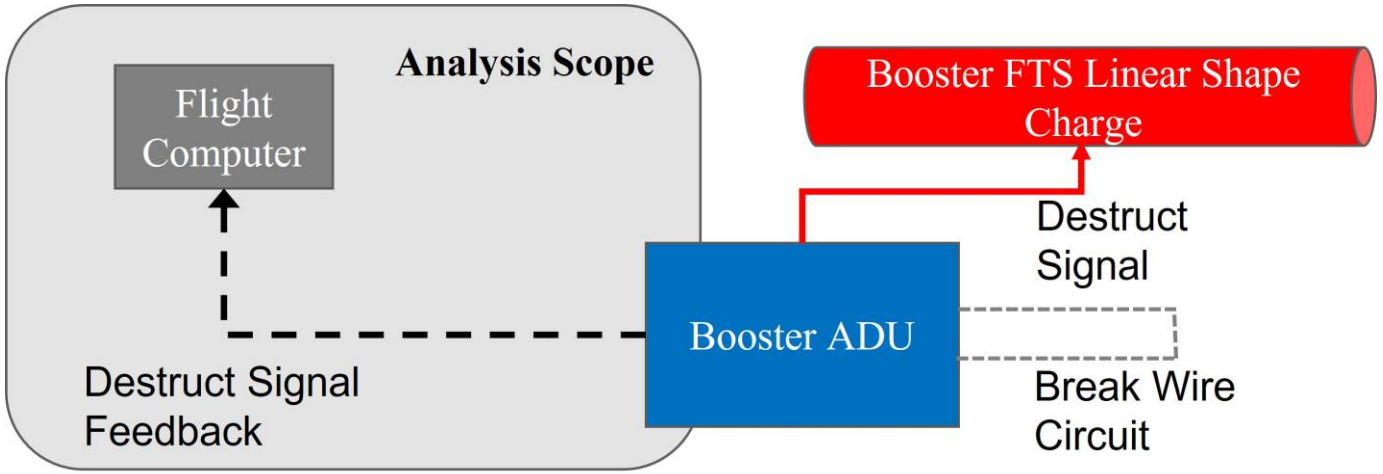
- External failures from the Orion, Interim Cryogenic Propulsion Stage element, ground support, flight control, or the crew.
- External monitoring functions (e.g., Launch Commit Criteria or Flight Rules)
- Effects of an underlying vehicle failure on the detection mechanism.

SLS FM Detection Risk Assessment Analysis Scope (continued 2/3)

The detection function risk assessment is based on measured property, not on the overall vehicle state.

Example – Booster Flight Termination System Activation Detection

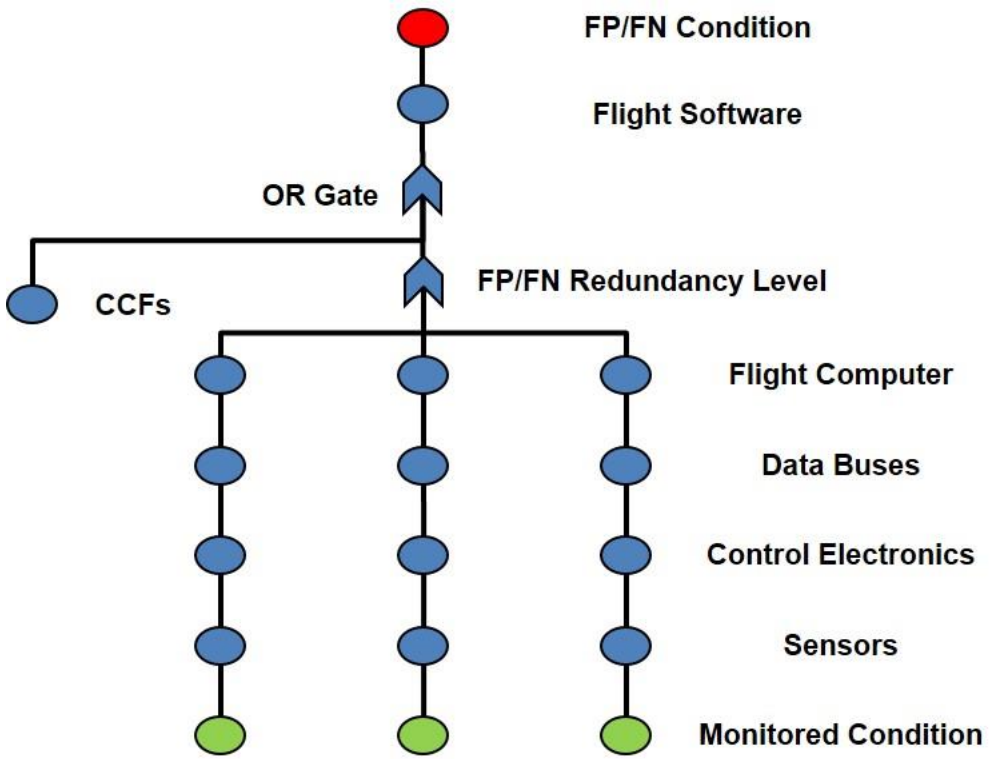
- Detects inadvertent Autonomous Destruction Unit (ADU) operation
- Failure of ADU/Break Wire Circuit result in a False Abort, but not a FP detection



SLS FM Detection Risk Assessment Analysis Scope (continued 3/3)

- Fault Tree logic developed along signal propagation paths
- Components involved:
  - Sensors,
  - Data and/or power buses,
  - Avionics boxes including computers, and software.
- Common Cause Failures (CCFs) modeled

Notional Fault Tree Representation



SLS FM Detection Risk Assessment Analysis Process

Hardware Components

- Failure probability models represent components under continuous operation, $P_{f_{hardware}}$
- Assume constant failure rate during operational phase, λ_0
- Analysis period, *t*, is small compared to Mean Time To Failure (MTTF)

$$P_{f_{hardware}} = 1 - e^{-\lambda_0 t} \cong \lambda_0 t$$

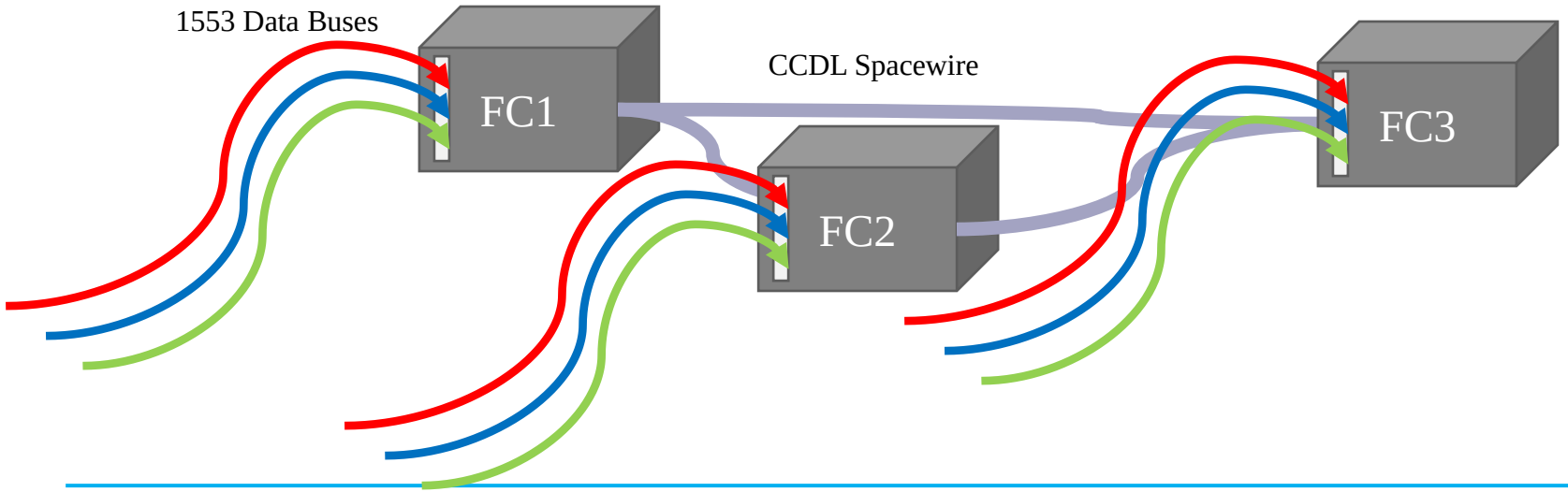
- Assessment required below box-level to determine failures likely to impact signal data
- Included CCF Modeling, Global Alpha Factor (GAF), Y_{GAF}, for redundant components

$$P_{f_{CCF}} = \lambda_0 * Y_{GAF} * t$$

SLS FM Detection Risk Assessment Analysis Process (continued 2/4)

Software

- Identical copies of the code are loaded into all three flight computers (FCs).
- Incoming data unique (often redundant) to each FC is qualified, exchanged between the FCs (ensure all are operating with identical data)



SLS FM Detection Risk Assessment Analysis Process (continued 3/4)

Software (continued)

- Software Modeling
  - Source Line Of Code (SLOC) as the smallest increment of source code that can be compiled into executable code by a compiler
  - Initial mission SW failure rate based on Shuttle data
  - Each SLOC was treated as independent with a constant identical failure rate, FR_{SW}.
    - Software analysis does not include code dependencies as the data did not support it.

$$P_{f_{software}} = FR_{SW} \times N_{SLOC}$$

  - Software risk estimations are treated as CCFs

SLS FM Detection Risk Assessment Analysis Process (continued 4/4)

Firmware Modeling

- Firmware is embedded code within a hardware component that is executed.
- The firmware risk estimation is modeled the same as software.
- Distinct from Field-Programable Gate Arrays (FPGAs) which are treated as hardware.
- Only three (3) avionics boxes identified containing firmware in the vehicle

SLS FM Detection Risk Assessment Analysis Refinements

Initial FP risk estimates resulted in excessive domination of software and firmware risk estimations.

1) Establishing software function traces for each detection algorithm
   - Traces included all signal processing code for signals used in detection logic (e.g. Data validation)
2) Utilizing the Logical Software Lines of Code (LSLOC) count
   - Counts focus on the executable portion of the software
   - Reduce sensitivity to coding styles and formatting

SLS FM Detection Risk Assessment Analysis Refinements (combined)

3) Refinement of the software failure rate
   - Softrel Frestimate Predictor software reliability tool
   - Inputs include total time under test and total found defects in each software version release

4) Established split values for common failures across fault trees
   - Direct Impact – failures that affect multiple detection functions
   - Exclusive Impact – failures that could result in unique outcomes (e.g. FP or FN outcome)

Summary & Conclusion

- Implementation of the analysis refinements
  - Provided more reasonable comparison of software and hardware risks.
  - Enabled risk assessments of the individual detection functions, while allowing assessment of the entire detection suite minimizing over-estimation.
- For Artemis II risk assessment, completed
  - All Abort Detection Functions FP/FN
  - Most Safing Detection Functions FP/FN
  - Warning Detection Functions FP only
- Results supported
  - Artemis II SLS Design Verification Objectives (DVOs)
  - Estimation of Artemis II overall LOC and LOM risks

Next Steps and Future Work

- How to capture redundancy in the software models.
- Standardize the firmware modeling throughout the Artemis program.
- Representation of software risk as an on-demand or a continuous element.
  - Incorporate time into software risk estimation representing the monitoring period